UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/664,613 | 09/17/2003 | Sean J. Mullan | SUN03-06(P9621) | 4049 |

58408 7590 11/02/2007

BARRY W. CHAPIN, ESQ.
CHAPIN INTELLECTUAL PROPERTY LAW, LLC
WESTBOROUGH OFFICE PARK
1700 WEST PARK DRIVE
WESTBOROUGH, MA 01581

| EXAMINER | |
|---|---|
| CHAI, LONGBIT | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 11/02/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/664,613 | MULLAN ET AL. | |
| | Examiner | Art Unit | |
| | Longbit Chai | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *14 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-4,6-20 and 22-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-20 and 22-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Presently, the pending claims are 1 – 4, 6 – 20 and 22 – 34.

### *Continued Examination Under 37 CFR 1.114*

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/14/2007 has been entered.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1 – 4, 6 – 16, 20 and 22 – 34 are rejected under 35 U.S.C. 102(e) as being anticipated by Bowe et al. (U.S. Patent 2003/0093678).

As per claim 29, Bowe teaches method for transmitting data in a network system according to a signature based protocol comprising:

identifying, at a server, data adapted for cryptographic transmission (Bowe: Abstract);

computing a digest on the identified data, the digest substantially indicative of the identified data (Bowe: Para [0132] Line 8);

building, according to a cryptographic scripting language (Bowe: Para [0019] and Para [0071] – [0074]: XML used as a cryptographic scripting language), a signature block, the signature block having a signed data portion, a signature value portion, a key information portion, and at least one information object portion, the signature value portion operable to store the signature as an authentication indicator according to the predetermined protocol, further comprises storing the signature in the signature value portion (Bowe: Para [0019], Para [0038] / Para [0072] and Para [0074]: XML used between the client signature request and Server signature response is considered as the predetermined protocol);

storing the identified data in the signed data portion of a signature block (Bowe: Para [0019], Para [0038] / Para [0072] and Para [0074]: signed object that also contains either the address of the signed object or contains the original object and the signature);

retrieving, from a public key infrastructure (PKI) a public and private key pair operable for cryptographic operations (Bowe: Para [0023], Para [0074] and Para [0139]: the KeyInfo element can contain a X509 data element so that the client can retrive the public key from it);

generating, at a server, a signature value from the private key corresponding to the computed digest, the signature substantially unrecreatable by data other than the computed digest (Bowe: Para [0035] and Para [0037]);

storing the signature value in the signature value portion of the signature block, the signature value portion and corresponding signature value persisting as a signature block according to the predetermined protocol including the payload data portion (Bowe: Para [0019], Para [0038] / Para [0072] and Para [0074]: signed object that also contains the original object (i.e. payload data) and the signature);

storing the public key corresponding to the private key in the key information portion to provide a self-authenticating transmission (Bowe: Para [0023] / Para [0139] and Para [0074]: the KeyInfo element can contain a X509 data element so that the client can retrieve the public key from the certificate for verification purpose); and

transmitting, according to the predetermined protocol, the signature block to a client also conversant in the scripting language and operable to store payload data in the information object portion independently of the signature value portion, storing in the information object portion further comprises storing the payload data at a client (see above), the client being unencumbered by signature generation operability (Bowe: Para [0035] and Para [0037]), the signature block being a script having fields defined by a predetermined metalanguage syntax (Bowe: Para [019] and Para [0071] – [0074]: XML itself used between the client signature request and Server signature response is indeed a predetermined metalanguage – This is consistent with the disclosure of the instant specification (SPEC: Page 17 / 1st Para / Line 6 – 8), the metalanguage syntax defining the position of the covered data portion (Bowe: Para [0072]: the address / position of the data to be signed (i.e. to be covered)), and corresponding signature, the signature block receivable by a recipient device conversant in the predetermined metalanguage syntax for decoding the message (Bowe: Para [0019] and Para [0071] – [0074]: signed object that also contains the original object (i.e. payload data) and the signature).

As per claim 1, 10, 20 and 32 – 34, the claim limitations are met as the similar reasons as that set forth above in rejecting claim 29.

As per claim 2 and 11, Bowe teaches the signature block further includes a signature value portion, the signature value portion operable to store the signature as an authentication

indicator according to the predetermined protocol, wherein storing further comprises storing the signature in the signature value portion (Bowe: Para [0019], Para [0038] / Para [0072] and Para [0074]: signed object that also contains either the address of the signed object or contains the original object and the signature).

As per claim 3, 12 and 22, Bowe teaches the signature block further includes a key information portion, further comprising storing an authentication indicator to a validation instrument in the key information portion, the validation instrument operable to authenticate the signature value portion using the signature (Bowe: Para [0023] and Para [0074]: the KeyInfo element can contain a X509 data element so that the client can retrive the public key from it).

As per claim 4 and 23, Bowe teaches the validation instrument corresponds to an inverse operation of the generating of the signature (Bowe: Para [0023] / Para [0139] and Para [0074]: the KeyInfo element can contain a X509 data element so that the client can retrieve the public key from the certificate for verification purpose).

As per claim 24, Bowe teaches storing in the information object portion further comprises storing the payload data at a client, the client being unencumbered by signature generation operability (Bowe: Para [0035] and Para [0037]).

As per claim 6 and 25, Bowe teaches storing the payload data further comprises generating a transmission block conformant with the predetermined protocol and operable to be received as a signature authenticated transmission by a destination node according to the predetermined protocol (Bowe: Para [0019], Para [0038] / Para [0072] and Para [0074]: XML

used between the client signature request and Server signature response is considered as the predetermined protocol).

As per claim 7 and 26, Bowe teaches generating the signature further comprises generating a signature corresponding to the covered data portion of the signature block (Bowe: Para [0019], Para [0038] / Para [0072] and Para [0074]: signed object that also contains the original object (i.e. payload data) and the signature).

As per claim 8 and 27, Bowe teaches computing a digest on the covered data portion, the digest substantially indicative of the data in the covered data portion (Bowe: Para [0132] Line 8).

As per claim 9 and 28, Bowe teaches the validation instrument is a public key and generating the signature further comprises generating a signature using the private key corresponding to the public key (Bowe: Para [0139]).

As per claim 13, Bowe teaches the receiving is performed by a nonsigning client which does not compute the signature and is unencumbered by components operable to compute the signature (Bowe: Para [0035] and Para [0037]).

As per claim 14, Bowe teaches indexing a remote signature repository, and the client is further operable to store the received signature in the signature block according to the predetermined protocol (Bowe: Para [0019], Para [0038] / Para [0072] and Para [0074]: XML

used between the client signature request and Server signature response is considered as the predetermined protocol).

As per claim 15, Bowe teaches receiving an authentication instrument corresponding to the signature, and storing the received authentication instrument in the signature block with the signed information portion and the signature (Bowe: Para [0019], Para [0038] / Para [0072] and Para [0074]: signed object that also contains the original object (i.e. payload data) and the signature).

As per claim 16, Bowe teaches the received authentication instrument is a public key corresponding to the private key for generating the signature, and storing further comprising forming a self-signed message by storing the public key in the key information portion (Bowe: Para [0023] / Para [0139] and Para [0074]: the KeyInfo element can contain a X509 data element so that the client can retrieve the public key from the certificate for verification purpose).

As per claim 30, Bowe teaches the scripting language is operable to incorporate signature components such that the scripting language is operable with signing capability when signature components are available and operable without signing capability when signature components are unavailable, further comprising:

identifying the signature value portion from a subset of available fields in the signature block, the signature value corresponding to the identified subset and the remaining available fields independent of the signature value (Bowe : Para [0019]);

identifying, from the remaining available fields, payload data portions operable for subsequent storage of data independent of the signature value and the signature value portion,

the payload data portions operable to be modified by subsequent recipients, wherein the signature value portion and corresponding signature value persist as a signature block according to the predetermined protocol including the payload data portions (Bowe: Para [0038] and Para [0072]: the original data object / payload is returned back to the client who has the ownership to manage the object).

As per claim 31, Bowe teaches a system for signature use by a nonsigning client generating, at a server, the nonsigning client unencumbered from cryptographic operation components, comprising:

at the client, identifying payload data adapted for storage in the information object portions according to the scripting language independent of the signature value (Bowe: Para [0019] and Para [0071] – [0074]: XML I used as a cryptographic scripting language); and storing the identified payload data in the information object portions in a nondestructive manner, the nondestructive manner operable to preserve the covered data portion (Bowe: Para [0019], Para [0038] / Para [0072] and Para [0074]: signed object that also contains the original object (i.e. payload data) and the signature) and corresponding signature without regenerating the signature, the client unencumbered and inoperable to encrypt and decrypt the signed data (Bowe: Para [0035] and Para [0037).

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are

such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 17 – 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bowe et al. (U.S. Patent 2003/0093678), in view of Kato et al. (U.S. Patent 2002/0040431).

As per claim 17, Bowe teaches at the nonsigning client, a plurality of signatures and corresponding covered data portions (Bowe : Para [0035] and Para [0037]). However, Bowe does not expressly teach selecting a first signature for inclusion in a first signature message for transmission to a destination recipient; selecting a second signature different than the first signature for inclusion in a second signature message for transmission to the same destination recipient.

Kao teaches selecting a first signature for inclusion in a first signature message for transmission to a destination recipient; selecting a second signature different than the first signature for inclusion in a second signature message for transmission to the same destination recipient (Kato : Para [0066] and Para [0080]: (a) a destination application is qualified as a destination recipient (b) more than one signature target information can be included in the same XML signature block S).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kato within the system of Bowe because Kato teaches a more convenient mechanism for XML signatures so that a plurality of signatures associated with XML documents can be provided under management in accordance with signature requests from the clients (Kato: Para [0026]).

As per claim 18, Bowe as modified teaches selecting the first and second signatures is performed based on signature selection logic, the signature selection logic for analyzing the covered data portion and the information object portion of the signature message to select an expected signature result at the destination recipient (Kato : Para [0079] and Para [0080]: the selected covered data portion is the selected signature target information with respect to the associated digital content).

As per claim 19, Bowe as modified teaches the signature selection logic is operable for analyzing the covered data portion based on at least one of the content type, size, creation date, and sparsity of the data (Kato : Para [0079] and Para [0080]: the selected covered data portion is the selected signature target information with respect to the associated digital content, which is qualified as sparsity of the data – i.e. not the entire payload data content).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Patent Examiner
Art Unit 2131
10/21/2007